



# PatrOwl

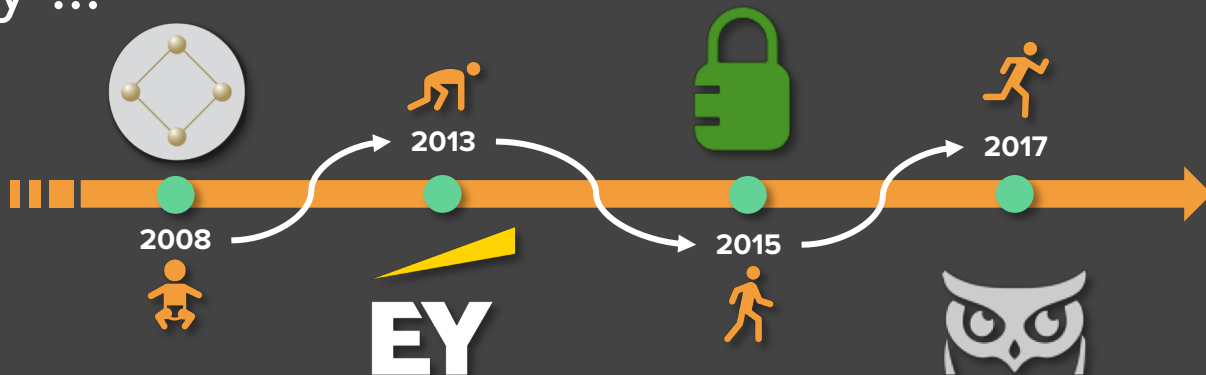
## Automation and Orchestration of Security Operations

#SOAR #OpenSource #PreventiveSecurity  
2019.03.23

## Yet another guy ...



**Nicolas MATTIOCCO**  
**@MaKyOtOx**  
**33 y/o** 🇫🇷



- ▶ Freelancer security auditor
- ▶ Currently onboarded in the **Red Team** of an internal CERT/CSIRT for a financial institution in France
- ▶ First-timer on an OSS project
- ▶ Proud dad (first-timer too)

*You don't even ~~care~~ need to know more about me...*

# My own definition of *SecOps* ©



# What is PatrOwl ?

Open source, integrated and scalable platform for SecOps automation and orchestration:

- **Continuous** and **full-stack** security overview
- Define threat intelligence & vulnerability assessment scans policies
- Orchestrate scans using tailor-made engines
- Collect & aggregate findings
- Contextualize, track and prioritize findings
- Check fixes and remediation effectiveness

## End-Users:

- CERT/SOC, CTI, DFIR, Penetration testers, Risk Manager, Internal Audit, CISO, Fusion Center
- CTO, Dev[Sec]Ops, Network and system engineers, QA, Developers
- M&A, Compliance teams, IssurTech





■ A new deadly tool ! But we missed some details...

Story **horse** ?



# Facing current and future cyber-security challenges

## Trends

**Assets exposed**



**Threats**

Vulnerabilities | Attackers |  
Security incidents



**Business impacts**  
of security incidents



## Facts & Challenges

1. **Poor visibility** on Cyber-exposure risks: Need to monitor a large, diversified, unmanaged and complex scope, even others assets ;
2. **Scarcity** of skilled and efficient **resources** in cyber-security ;
3. **Windows of exposure problem**: Cyber-security mediatisation causes high visibility for vulnerabilities and easiness of attacks ;
4. **Tool capacity-based approach** rather a business threats-based approach. Our great security tools are ineffective without proper strategy, expertise and processes.

**Cyber-Exposure and risks are continuously growing and quickly changing**



# Facing current and future cyber-security challenges

## Security Incident Management

**Precursores** (may occur)

**Indicators** (have occurred or is happening)

**Events monitoring** reveals vulnerabilities and suspicious changes

### Asset updates

- Application, system or network updates
- Infrastructure changes: open/closed ports, new subdomain, IP or domain assignment
- Shadow IT ?

### Infosec KB updates

- CVE, CVSS, CPE updates
- 0-days & misc.
- Exploit releasing
- New detection method: scanner update, new tool released, policy updates, infosec researches
- Publication of IOCs

### Ext. resource updates

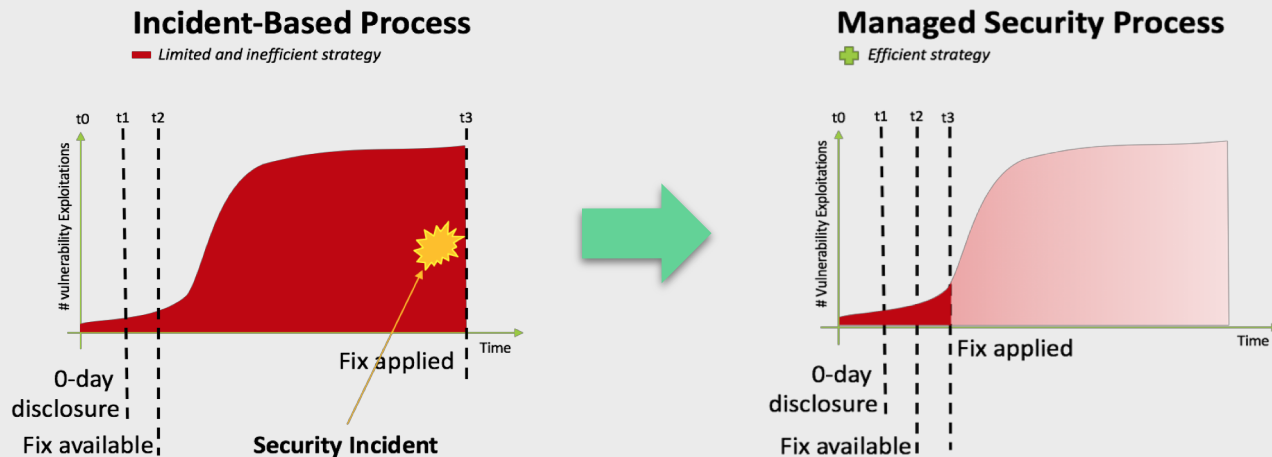
- Data leaks
- Fraud: IP or DNS blacklists, Malware analysis, Typosquatting, ...
- Phishing campaign
- Changes on potential attackers' assets
- Attacks announcements
- Suspicious activities (SIEM)



# Facing future cyber-security challenges



The “Window of Exposure” problem



***Proactive detection  
+ Alert notification  
= Early fixing  
= Safe earlier  
(QED)***

**Attackers will attack your assets.  
Tackling the window of exposure is now a top priority.**



How to face these bigger, better, badder threats ?

What about  
**Automation** and  
**Orchestration** ?



How to face these bigger, better, badder threats ?



# Why automating SecOps ?

## Do **more** checks

- Cover a larger and diversified scope
- Empower new capacities and improve cyber-security maturity level
- Get a better overview of cyber-exposure (full-stack)

## Do it more **efficiently**

- Reduce low value-adding tasks to focus on more complex security cases
- Reduce and manage costs
- Assess effectiveness of your SecOps activities through measurable KPIs



## Do it more **often**

- Check continuously for vulnerabilities and suspicious changes
- Reduce delays in discovering and fixing a security incident (vulnerability or pwnage)
- Keep updated of your cyber-exposition risks

## Do **compliance** and **benchmarks**

- Define and expedite controls
- Assess compliance level regarding corporate, regulatory and statutory standards
- Benchmark security level of assets using same control policies

**AUTOMATION**



**PLEASE TAKE MY JOB**





## Of course, there are several known limits...

It does not cover 100% of risks in itself (do not be so naïve... Black magic does not exist)

**Number of alerts ?**

**False-Positives ?**

**Functional vulnerabilities ?**

**Qualification &  
Contextualisation ?**

**Total Costs of Ownership ?**

**Cyber-Defence Strategy ?**

... and probably all others generic downsides of automated systems ...



SecOps automation as a new standard ?

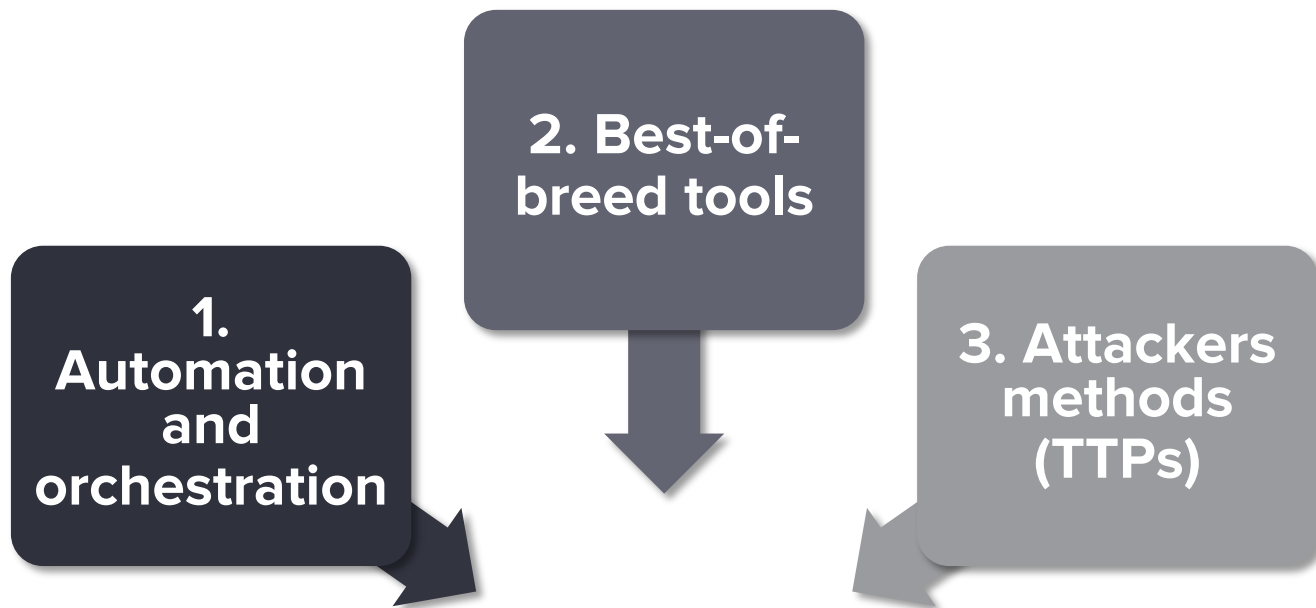
BTW, we built **PatrOwl**  
for automating and  
orchestrating **SecOps**





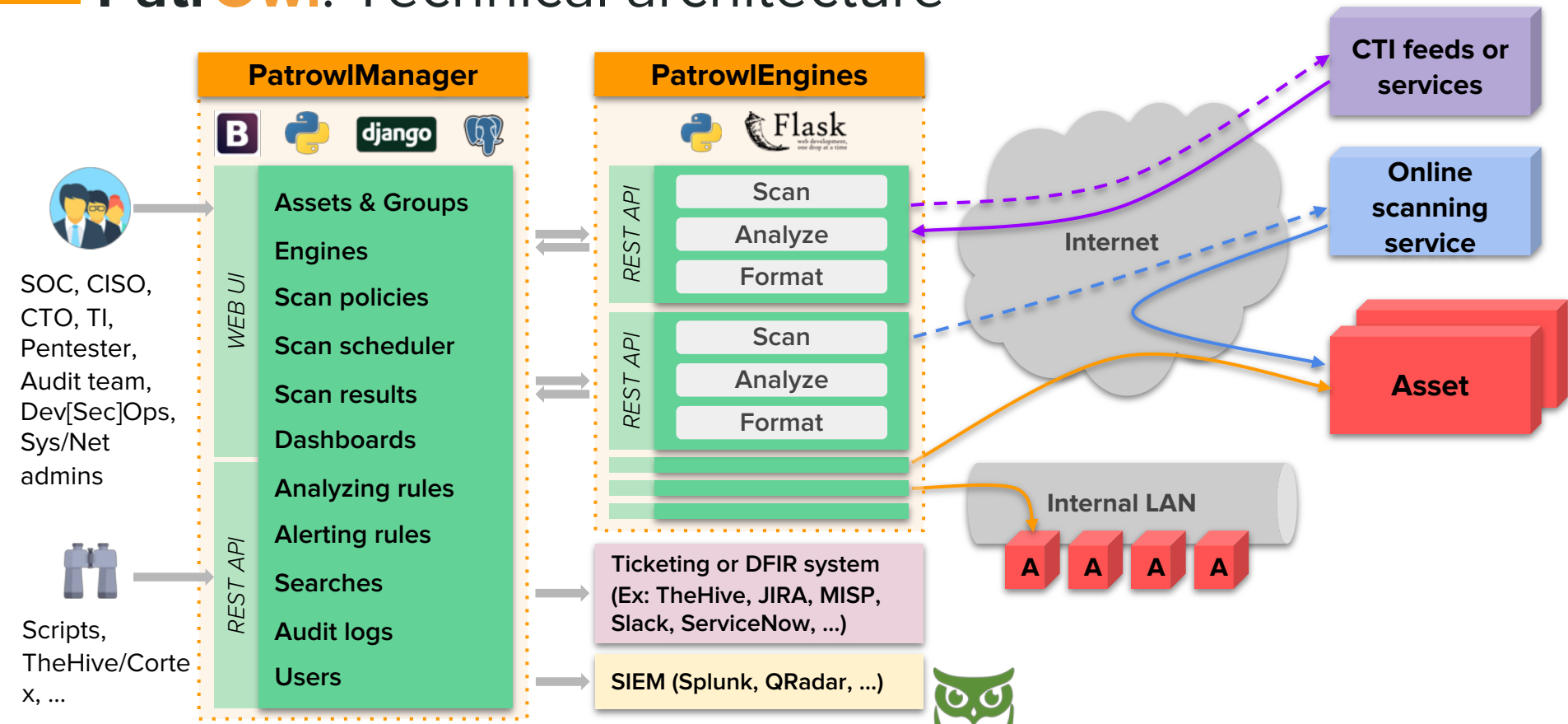
# PatrOwl's incentives

Efficiently moving from a reactive to a more predictive security posture with:



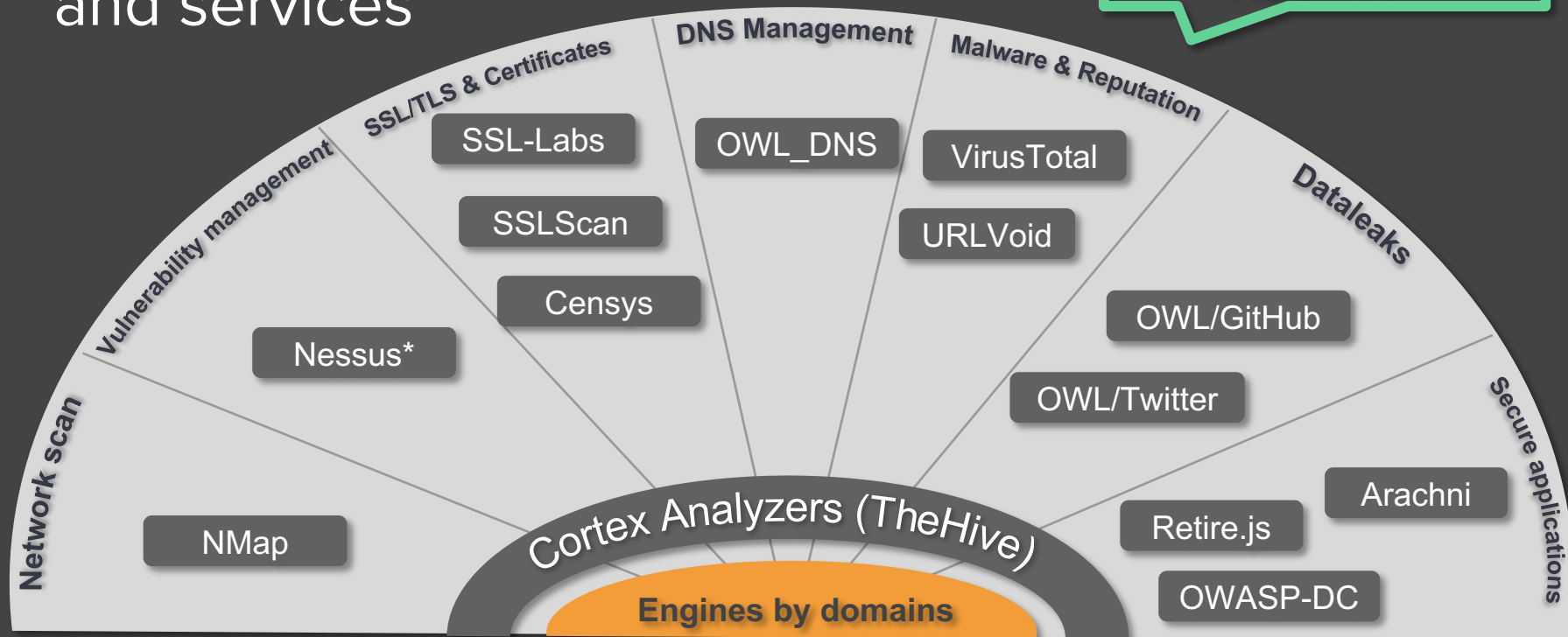
*Wut !?! Feeling spotted now...*

# PatrOwl: Technical architecture



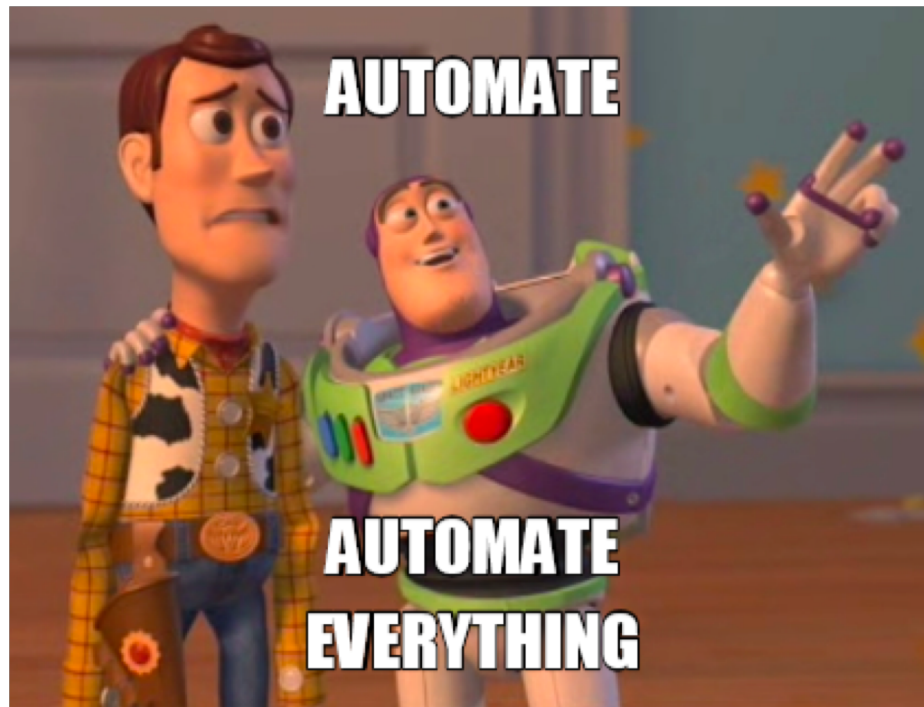
# PatrowlEngines: Supported tools and services

**Turnkey** micro-apps:  
Docker images +  
REST-API



## Next engines in the pipeline (to be confirmed)

- **Vulnerability management:**  
OpenVas, Qualys, Rapid7 IVM
- **Pasties:** CIRCL-AIL
- **CTI:** MISP, Shodan.io
- **WEB:** Acunetix, Burp, WPScan, DroopScan
- **Containers:** AquaSec, CLAIR (CoreOS), Jfrog Xray
- **Dataleaks:** Git/truffleHog
- **Cloud:** Scout2, CloudSploit
- ... Any other idea ?



# Various use cases

## Data leaks

Monitor code leaks on GitHub, sharing platforms (Pasties), emails in dump leaks, open AWS buckets, ...

## Vulnerability and remediation tracking

Identify vulnerabilities, send a full report to ticketing system (TheHive, JIRA, ...) and rescan to check for remediation

## Vulnerability assessment

Orchestrate regular scans on a fixed perimeter, check changes (asset, vulnerability, CVSS, available exploits)

## Monitoring attacker or suspicious assets

Ensure readiness of teams by identifying attackers' assets and tracking changes of their IP, domains, WEB applications

## Monitoring Internet-facing systems

Scan continuously websites, public IP, domains and subdomains for vulnerabilities, misconfigurations, ...

## Phishing / APT scenario preparation

Monitor early signs of targeted attacks: new domain registration, suspicious Tweets, suspicious pasties, VirusTotal submissions, phishing reports, ...

## Regulation and Compliance

Evaluate compliance gaps using tailor-made scan templates

## Penetration tests

Perform the reconnaissance steps, the full-stack vulnerability assessment and the remediation checks

## Securing the CI / CD pipeline

Automation of static code analysis, external resources assessment and web application vulnerability scans





# Take-away



## Cost-Effective

Rationalize tools integration, product licenses and skills



## Time-To-Value

Ease of use and deployment, templates for scan policies



## Adaptability & Scalability

REST API, Open-Source connectors, adaptable to organisation's ecosystems



## 360° overview

Full-stack assessment of cyber-exposure, in real-time with relevant data



## Always updated

Vulnerability KB, detection methods, threat scenarios



## Made with ❤️ by experts

Our team members are A+ security engineers



# We currently work on:

- **More integration with:**



**TheHive**



**RUDDER**

- Security Incident Response
- IT Automation and Continuous Configuration

- **Patrowl4py:** Python API client for PatrowlManager and PatrowlEngines

- **Testing various use cases**

- ~~Monetization!~~ **Exploring commercial opportunities:**

- **Premium features:** Enterprise authentication, custom dashboards & reports, dynamic assets sync, risk rating / scorecards, event correlation, multi-scans templates, premium engines, ...
- **Cloud/SaaS solution:** Hosted on a Kubernetes cluster. Ask us for a beta account !  
mailto: [getsupport@patrowl.io](mailto:getsupport@patrowl.io) or twits accepted ;)

- **Debugging and improving quality (endlessly)**

- **Documenting (endlessly too !) + scan templates**



# It's an open-source project: Contribution is needed !!

## Who's up for:

- **Testing it** and giving us lots of **feedbacks !**
- **Contributing:**
  - New engines
  - Debug
  - Features ??
- **Joining the core team ?**
- **Funding us ?**



*\* FR-EN translation hint: "Oui Nide lou" == "We Need You"  
Trust me, it's a veeery funny joke in french*

Dev[Sec]Ops,  
Security  
engineer, Cloud  
Architect, UX/UI  
Designer, QA  
Tester, Wonder-  
Woman  
(Batman is  
tolerated too) ...



## Q&A

**1 We have lots of  
questions !?!**

**2 We want a  
demo !?!**  
-- Meet us !

**3 Enough ! Please  
stop talking bro !?!**  
-- Thanks for the attention !

## Contacts

More details ? Meet us ? Contributing ? Want a demo ? Want an awesome sticker ? Share a beer ? Requesting an online/SaaS demo account (BETA test) ?

Find us everywhere on earth:

**Now:** Just in front of you

**Mail:** [getsupport@patrowl.io](mailto:getsupport@patrowl.io)

**Web:** <https://patrowl.io>

**Twitter:** [@patrowl\\_io](https://twitter.com/patrowl_io) (Follow us !)

**GitHub:** [@Patrowl](https://github.com/Patrowl) (Star and fork us !)

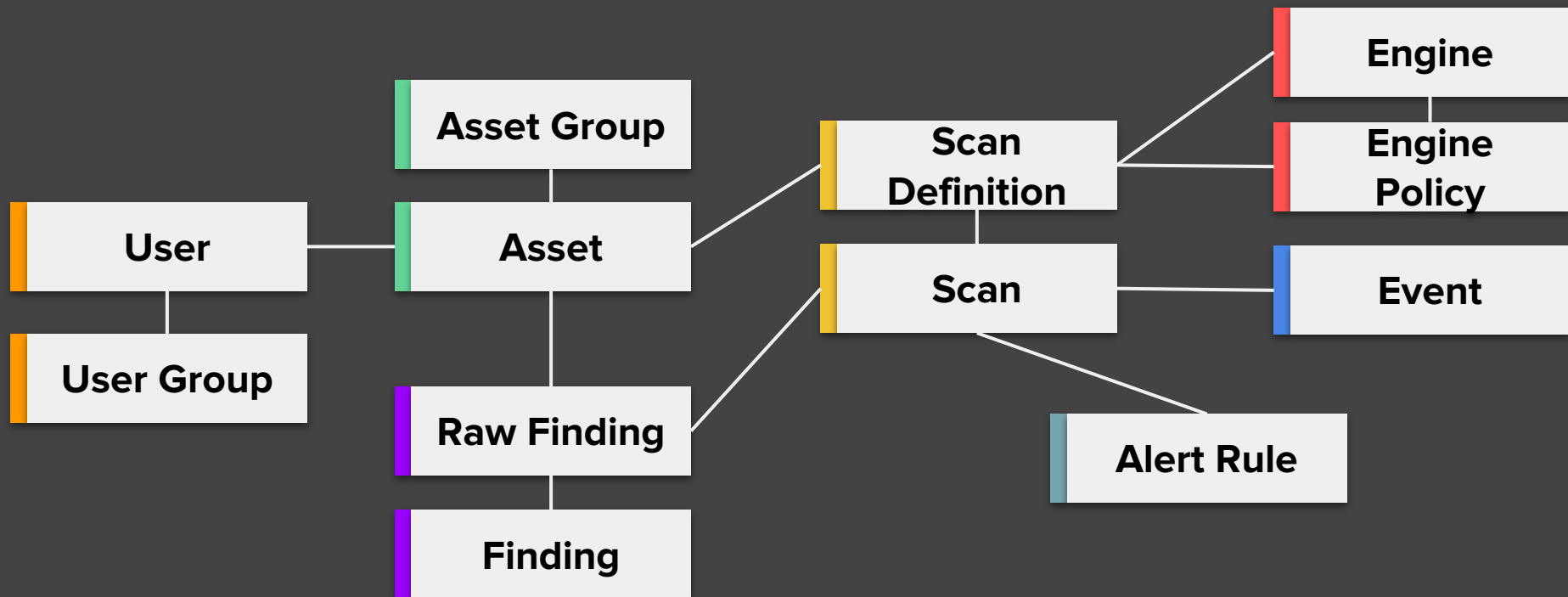
Before you ask: Why PatrOwl is named “PatrOwl” ?



- The owl is able to see in the dark ~~deep web~~ with a large peripheral vision (almost 360°)
- The domain “patrowl.io” name was not already registered



## Data Model (simplified)



# PatrOwl Manager - Dashboard

Global indicators on assets,  
findings, scans, engines and rules

Asset and asset group grades

Most vulnerabilities assets and asset  
groups

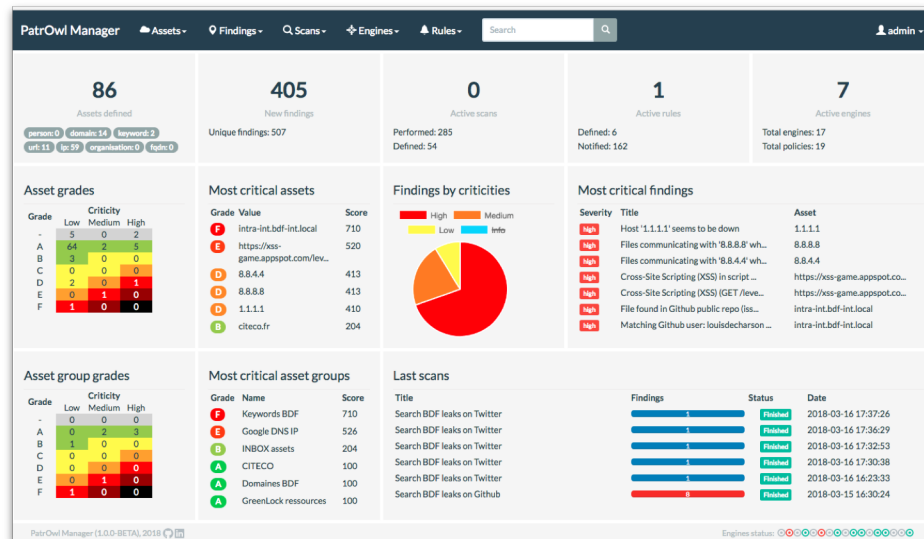
Most critical findings

Findings repartition by severity

Last scans status and results

Top CVSS Score / Findings

Top CVE, CWE, CPE, ...



100%

Current finding counters, risk grade and trends (last week, months, ...)

## Findings by threat domains:

- Domain, HTTPS & Certificate, Network infrastructure, System, Web App, Malware, E-Reputation, Data Leaks, Availability

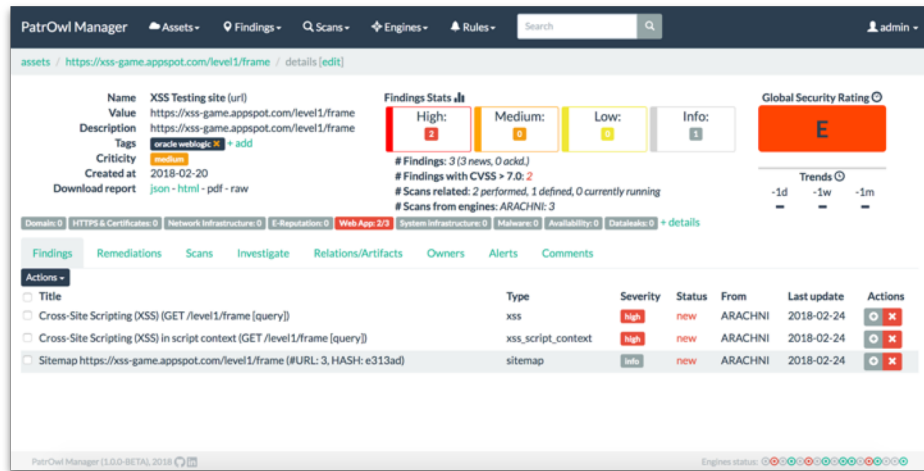
## All findings and remediations tips

## Related scans and assets

## Investigation links

## Export HTML, CSV or JSON reports

## Custom tags



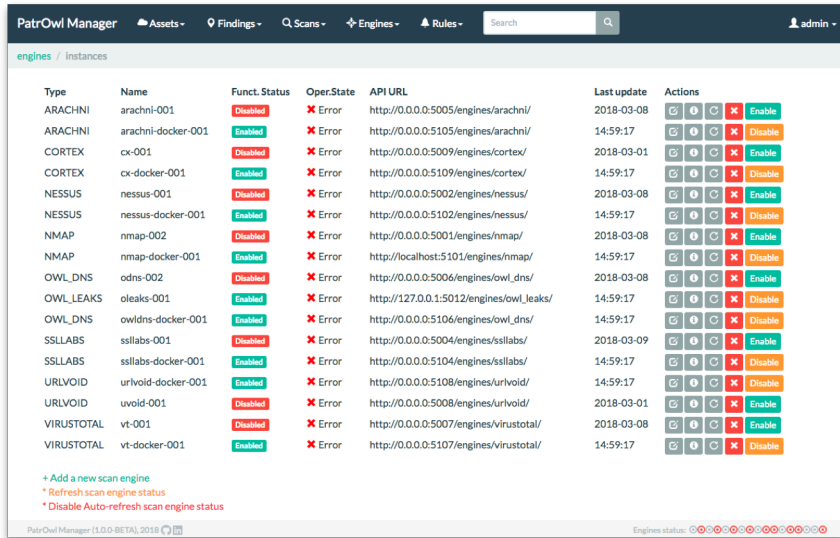


100%

## Change functional state

## Refresh engines states

## Enable/Disable the auto-refresh



Engines states are regularly updated and always shown in the footer:

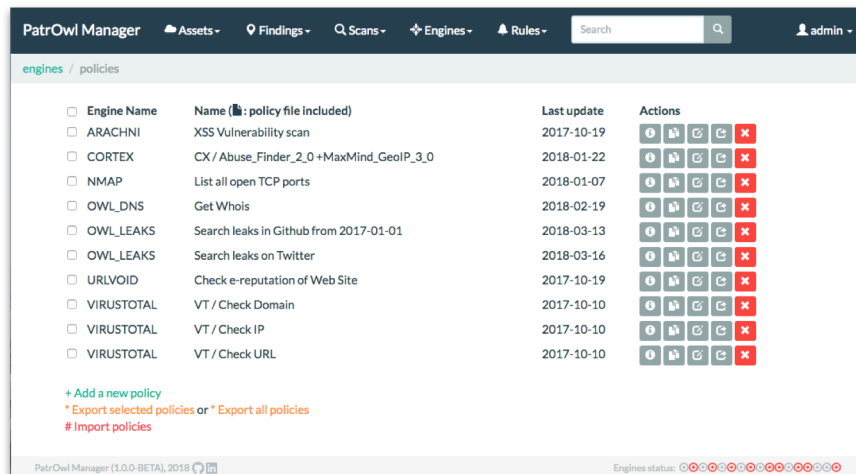
Engines status:



# PatrOwl Manager - Engine policy views

Create, copy, modify or delete  
engine policies

Quick policy info retrieving

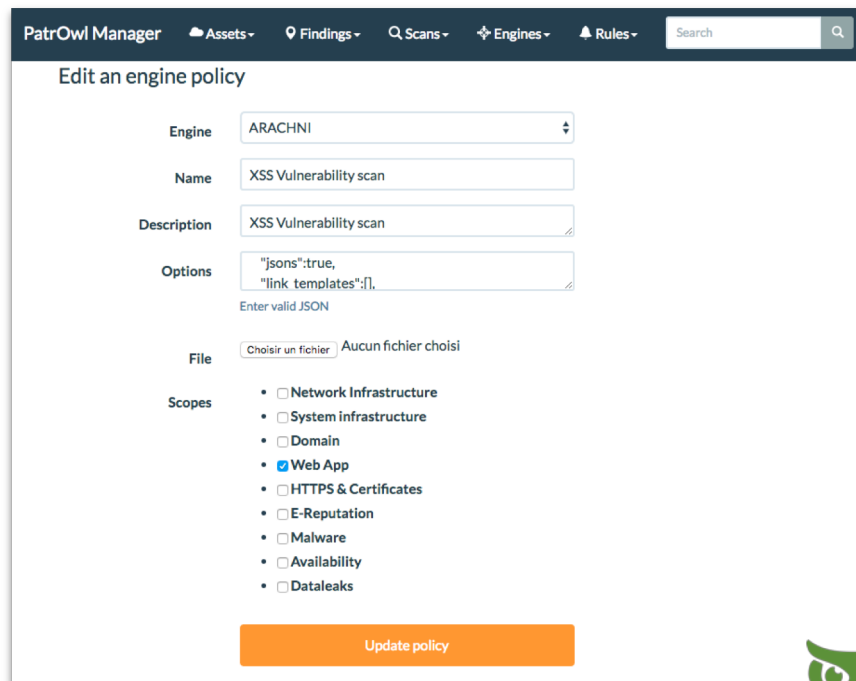


Engine Name	Name (policy file included)	Last update	Actions
ARACHNI	XSS Vulnerability scan	2017-10-19	[Icons]
CORTEX	CX / Abuse_Finder_2_0 +MaxMind_GeolP_3_0	2018-01-22	[Icons]
NMAP	List all open TCP ports	2018-01-07	[Icons]
OWL_DNS	Get Whois	2018-02-19	[Icons]
OWL_LEAKS	Search leaks in Github from 2017-01-01	2018-03-13	[Icons]
OWL_LEAKS	Search leaks on Twitter	2018-03-16	[Icons]
URLVOID	Check e-reputation of Web Site	2017-10-19	[Icons]
VIRUSTOTAL	VT / Check Domain	2017-10-10	[Icons]
VIRUSTOTAL	VT / Check IP	2017-10-10	[Icons]
VIRUSTOTAL	VT / Check URL	2017-10-10	[Icons]

+ Add a new policy  
\* Export selected policies or \* Export all policies  
# Import policies

PatrOwl Manager (1.0.0-BETA), 2018 Engines status: [Progress Bar]

Engine policy details:



PatrOwl Manager Assets Findings Scans Engines Rules Search

### Edit an engine policy

Engine: ARACHNI

Name: XSS Vulnerability scan

Description: XSS Vulnerability scan

Options: {"jsons":true, "link\_templates":[]}

Enter valid JSON

File: Choisir un fichier / Aucun fichier choisi

Scopes:

- ☐ Network Infrastructure
- ☐ System infrastructure
- ☐ Domain
- ☒ Web App
- ☐ HTTPS & Certificates
- ☐ E-Reputation
- ☐ Malware
- ☐ Availability
- ☐ Dataleaks

Update policy



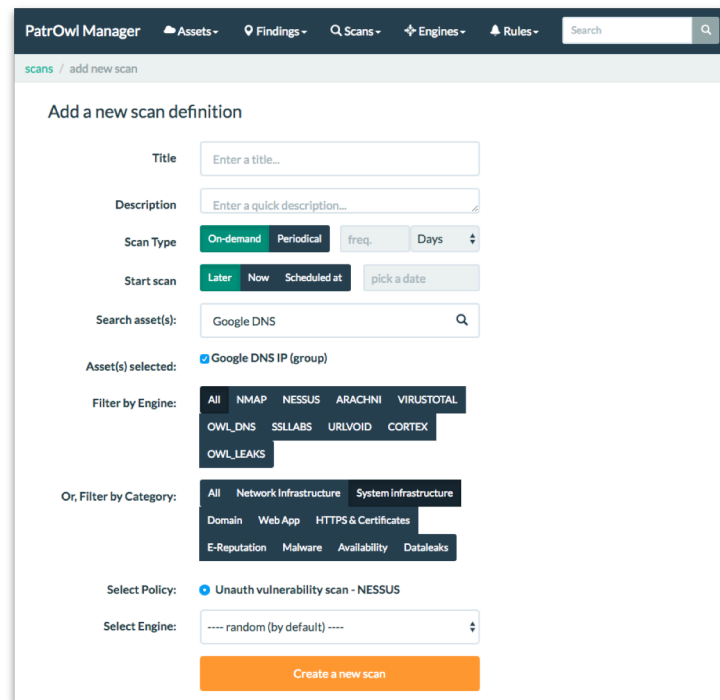
# PatrOwl Manager - Scan definition creation view

Search and select assets and asset groups on their value or name

Filter policies by engine type or threat domain

Select engine

- If no engine is selected, an engine is randomly chosen in available engines for each scan



The screenshot shows the 'Add a new scan definition' form in the PatrOwl Manager interface. The form includes the following fields and options:

- Title:** A text input field with the placeholder 'Enter a title...'.
- Description:** A text input field with the placeholder 'Enter a quick description...'.
- Scan Type:** A dropdown menu with options: On-demand (selected), Periodical, freq., and Days.
- Start scan:** A dropdown menu with options: Later (selected), Now, Scheduled at, and a 'pick a date' button.
- Search asset(s):** A search input field containing 'Google DNS'.
- Asset(s) selected:** A list of selected assets, currently showing 'Google DNS IP (group)'.
- Filter by Engine:** A list of engine filters: All (selected), NMAP, NESSUS, ARACHNI, VIRUSTOTAL, OWL\_DNS, SSLLABS, URLVOID, CORTEX, and OWL\_LEAKS.
- Or, Filter by Category:** A list of category filters: All (selected), Network Infrastructure, System Infrastructure, Domain, Web App, HTTPS & Certificates, E-Reputation, Malware, Availability, and Dataleaks.
- Select Policy:** A dropdown menu with the selected policy 'Unauth vulnerability scan - NESSUS'.
- Select Engine:** A dropdown menu with the selected engine '---- random (by default) ----'.
- Create a new scan:** An orange button at the bottom of the form.



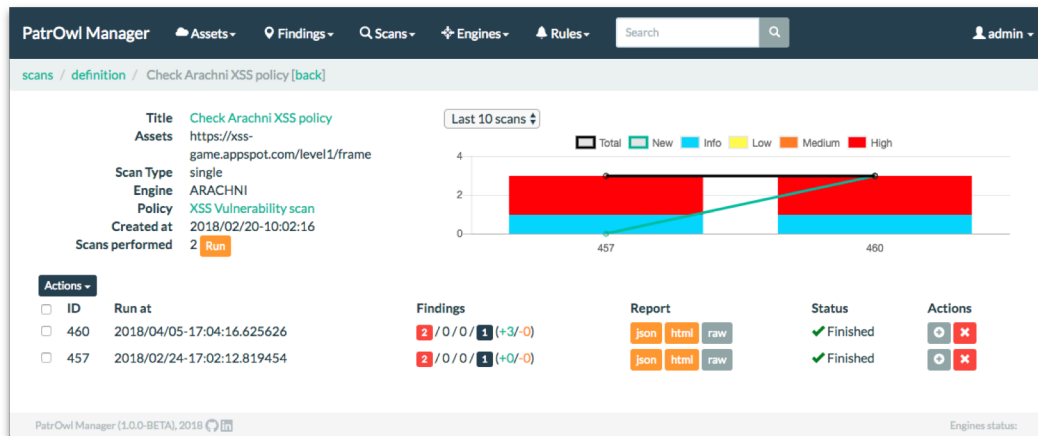
# PatrOwl Manager - Scan definition view

Related scan results overview

- ID, starting datetime, finding counters by severities, status

Quick run button

Quick scan report (HTML or JSON), delete or show details

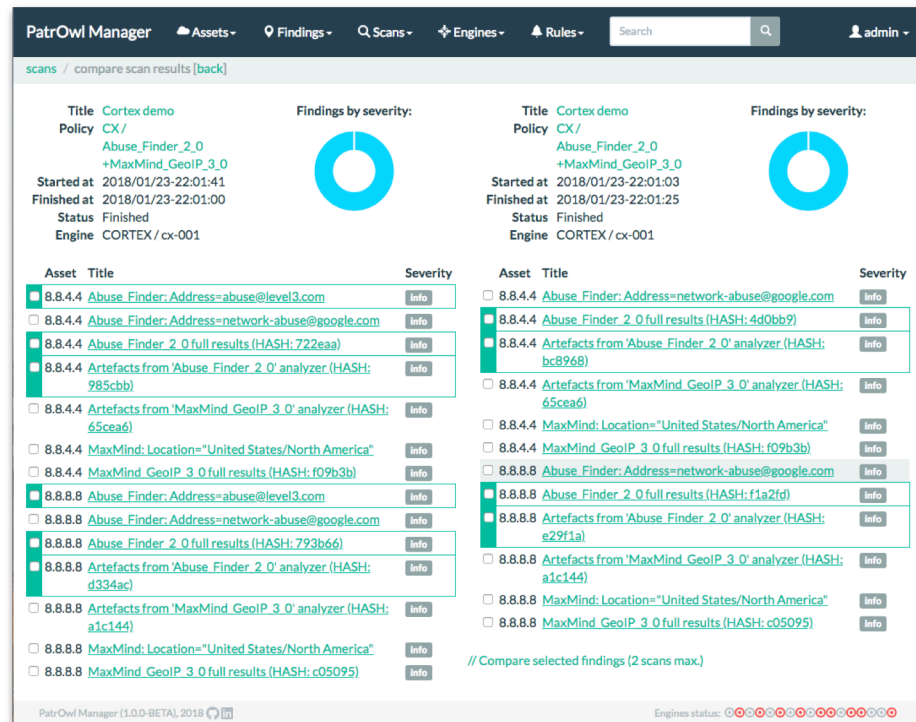


# PatrOwl Manager - Scan compare view

Highlighting differences:

- new and missing findings
- same finding type but different details

Link to the findings comparison view



PatrOwl Manager

Assets Findings Scans Engines Rules Search admin

scans / compare scan results [back]

**Title** Cortex demo  
**Policy** CX / Abuse\_Finder\_2\_0 +MaxMind\_GeoIP\_3\_0  
**Started at** 2018/01/23-22:01:41  
**Finished at** 2018/01/23-22:01:00  
**Status** Finished  
**Engine** CORTEX / cx-001

**Findings by severity:**


Asset	Title	Severity
<input checked="" type="checkbox"/>	8.8.4.4 Abuse_Finder: Address=abuse@level3.com	info
<input type="checkbox"/>	8.8.4.4 Abuse_Finder: Address=network-abuse@google.com	info
<input checked="" type="checkbox"/>	8.8.4.4 Abuse_Finder_2_0 full results (HASH: 722eaa)	info
<input checked="" type="checkbox"/>	8.8.4.4 Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: 985cbb)	info
<input type="checkbox"/>	8.8.4.4 Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: 65cea6)	info
<input type="checkbox"/>	8.8.4.4 MaxMind: Location="United States/North America"	info
<input type="checkbox"/>	8.8.4.4 MaxMind_GeoIP_3_0 full results (HASH: f09b3b)	info
<input checked="" type="checkbox"/>	8.8.8.8 Abuse_Finder: Address=abuse@level3.com	info
<input type="checkbox"/>	8.8.8.8 Abuse_Finder: Address=network-abuse@google.com	info
<input checked="" type="checkbox"/>	8.8.8.8 Abuse_Finder_2_0 full results (HASH: 793b66)	info
<input checked="" type="checkbox"/>	8.8.8.8 Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: d334ac)	info
<input type="checkbox"/>	8.8.8.8 Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: a1c144)	info
<input type="checkbox"/>	8.8.8.8 MaxMind: Location="United States/North America"	info
<input type="checkbox"/>	8.8.8.8 MaxMind_GeoIP_3_0 full results (HASH: c05095)	info

**Title** Cortex demo  
**Policy** CX / Abuse\_Finder\_2\_0 +MaxMind\_GeoIP\_3\_0  
**Started at** 2018/01/23-22:01:03  
**Finished at** 2018/01/23-22:01:25  
**Status** Finished  
**Engine** CORTEX / cx-001

**Findings by severity:**

Asset	Title	Severity
<input type="checkbox"/>	8.8.4.4 Abuse_Finder: Address=network-abuse@google.com	info
<input checked="" type="checkbox"/>	8.8.4.4 Abuse_Finder_2_0 full results (HASH: 4d0bb9)	info
<input checked="" type="checkbox"/>	8.8.4.4 Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: bc8968)	info
<input type="checkbox"/>	8.8.4.4 Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: 65cea6)	info
<input type="checkbox"/>	8.8.4.4 MaxMind: Location="United States/North America"	info
<input type="checkbox"/>	8.8.4.4 MaxMind_GeoIP_3_0 full results (HASH: f09b3b)	info
<input type="checkbox"/>	8.8.8.8 Abuse_Finder: Address=network-abuse@google.com	info
<input checked="" type="checkbox"/>	8.8.8.8 Abuse_Finder_2_0 full results (HASH: f1a2fd)	info
<input checked="" type="checkbox"/>	8.8.8.8 Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: e29f1a)	info
<input type="checkbox"/>	8.8.8.8 Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: a1c144)	info
<input type="checkbox"/>	8.8.8.8 MaxMind: Location="United States/North America"	info
<input type="checkbox"/>	8.8.8.8 MaxMind_GeoIP_3_0 full results (HASH: c05095)	info

// Compare selected findings (2 scans max.)

PatrOwl Manager (1.0.0-BETA), 2018 Engines status: 



# PatrOwl Manager - Scan results view

Scans info: title, assets, status, policy, start/end dates

Findings list + show details link

Quick scan report (HTML or JSON)

Findings summary on metrics

Asset and asset group overview

overview

List of related events

PatrOwl Manager Assets Findings Scans Engines Rules Search admin

scans / Check Arachni XSS policy [back]

Assets 1 Asset groups 0 Findings 3 Events 0

Asset	Finding Title	Status	Severity	Actions
https://xss-game.appspot.com...	Cross-Site Scripting (XSS) (GET /level1/frame [query])	new	high	
https://xss-game.appspot.com...	Cross-Site Scripting (XSS) in script context (GET /level1/frame [query])	new	high	
https://xss-game.appspot.com...	Sitemap https://xss-game.appspot.com/level1/frame (#URL: 3, HASH: e313ad)	new	info	

Scan details (ID=460)

Title: Check Arachni XSS policy  
Assets: https://xss-game.appspot.com...  
Engine: arachni-001 (ARACHNI)  
Status: Finished  
Policy: XSS Vulnerability scan  
Started at: 2018/02/24-17:02:55  
Finished at: 2018/02/24-17:02:39  
Elapsed: 0:00:43.152597  
Reports: [json](#) [html](#) [raw](#)

Findings summary

(A) CVSS > 7: 2  
(B) > 30 days: 3  
(A) + (B): 2

Repartition per severity:

High Medium Low Info

PatrOwl Manager (1.0.0-BETA), 2018 Engines status:



# PatrOwl Manager - Scan performed view

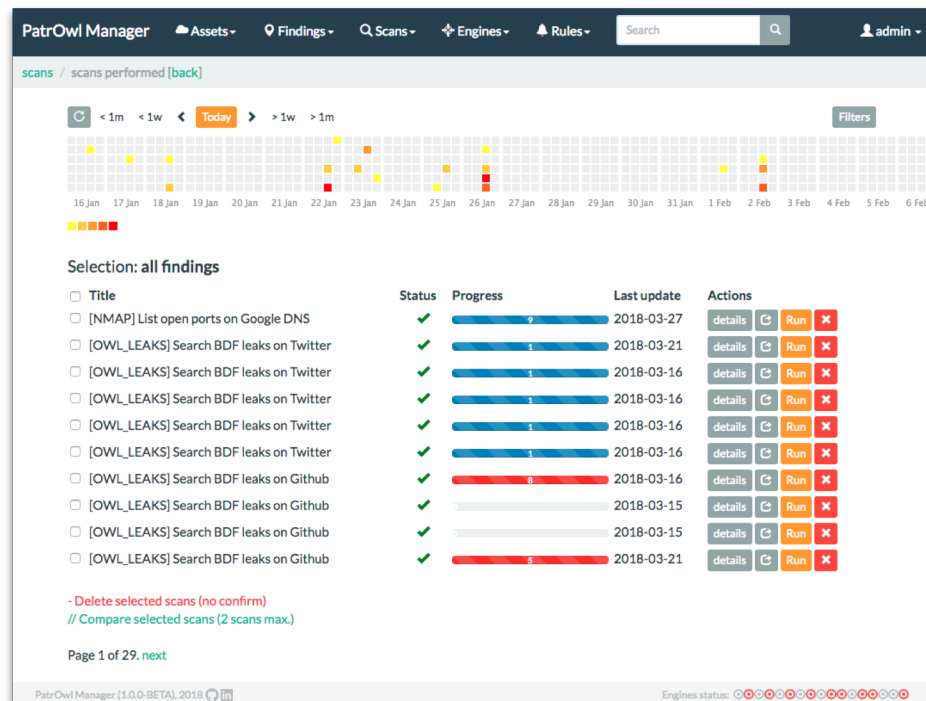
Scans heatmap over days, weeks and months

Advanced filters

Run or delete scans

Show scan details

Compare selected scans



# PatrOwl Manager - Finding view

## Finding info

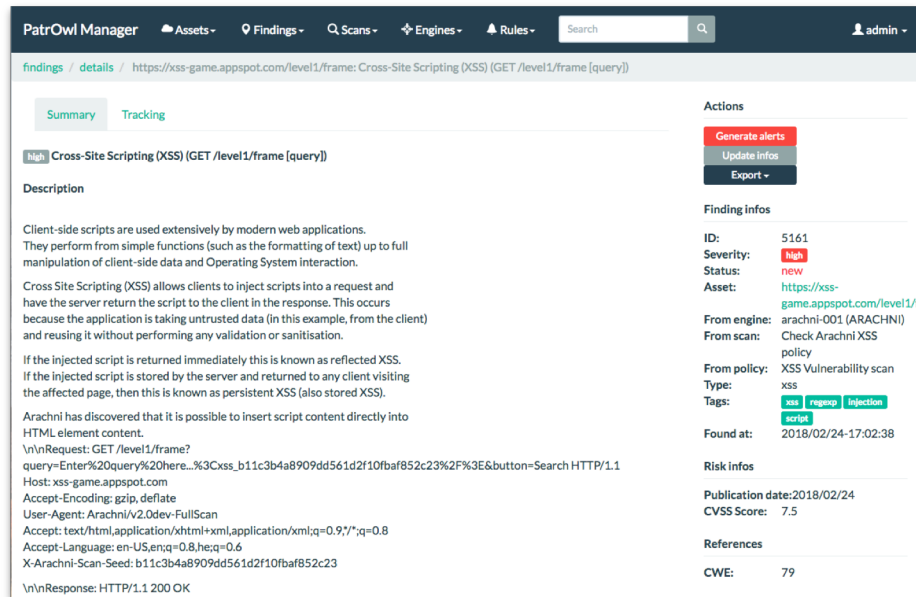
Description, solution, links and hash

## Quick actions:

- Generate alerts
- Change metadata: severity, status, tags, CVSS
- Export to file (JSON or STIX2 format)

## Show tracking info

- Changes history
- Matching scans



The screenshot displays the PatrOwl Manager web interface. The top navigation bar includes links for Assets, Findings, Scans, Engines, Rules, and a search bar. The user 'admin' is logged in. The main content area shows a finding titled 'Cross-Site Scripting (XSS) (GET /level1/frame [query])' with a 'High' severity. The finding is categorized under 'Summary' and 'Tracking'. The description explains that XSS allows clients to inject scripts into a request, which the server then returns to the client. It also mentions that Arachni has discovered it is possible to insert script content directly into HTML element content. The right sidebar contains 'Actions' (Generate alerts, Update info, Export), 'Finding info' (ID: 5161, Severity: High, Status: new, Asset: https://xss-game.appspot.com/level1/frame, From engine: arachni-001 (ARACHNI), From scan: Check Arachni XSS policy, From policy: XSS Vulnerability scan, Type: XSS, Tags: xss, rgroup, injection, script, Found at: 2018/02/24-17:02:38), 'Risk info' (Publication date: 2018/02/24, CVSS Score: 7.5), and 'References' (CWE: 79).

PatrOwl Manager Assets Findings Scans Engines Rules Search admin

findings / details / https://xss-game.appspot.com/level1/frame: Cross-Site Scripting (XSS) (GET /level1/frame [query])

Summary Tracking

**High** Cross-Site Scripting (XSS) (GET /level1/frame [query])

**Description**

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation.

If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS).

Arachni has discovered that it is possible to insert script content directly into HTML element content.

\n\nRequest: GET /level1/frame?  
query=Enter%20Query%20here...%3Cscript%3Ealert(1)&button=Search HTTP/1.1  
Host: xss-game.appspot.com  
Accept-Encoding: gzip, deflate  
User-Agent: Arachni/v2.0dev-FullScan  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9/\*;q=0.8  
Accept-Language: en-US,en;q=0.8,he;q=0.6  
X-Arachni-Scan-Seed: b11c3b4a8909dd561d2f10fbaf852c23  
\n\nResponse: HTTP/1.1 200 OK

**Actions**

Generate alerts  
Update info  
Export

**Finding info**

ID: 5161  
Severity: **High**  
Status: **new**  
Asset: https://xss-game.appspot.com/level1/frame  
From engine: arachni-001 (ARACHNI)  
From scan: Check Arachni XSS policy  
From policy: XSS Vulnerability scan  
Type: XSS  
Tags: **xss** **rgroup** **injection** **script**  
Found at: 2018/02/24-17:02:38

**Risk info**

Publication date: 2018/02/24  
CVSS Score: 7.5

**References**

CWE: 79







# PatrOwl Manager - Finding compare view


Highlighting differences  
between findings

PatrOwl Manager Assets Findings Scans Engines Rules Search admin

findings / compare [back]

	Finding A (ID: 1181)	Finding B (ID: 1179)
Title	Port 'tcp/80' is filtered	Port 'tcp/56' is filtered
Severity	info	info
Asset	8.8.8.8	8.8.8.8
Description	The scan detected that the port 'tcp/80' was filtered	The scan detected that the port 'tcp/56' was filtered
Solution	n/a	n/a
Risk info	vuln_publication_date: 2018/01/16 cvss_base_score: 0.0	vuln_publication_date: 2018/01/16 cvss_base_score: 0.0
Vuln info	n/a.	n/a.
Links	No links.	No links.
Tags	No Tags.	No Tags.
Created at	2018/01/16-12:01:32	2018/01/16-12:01:30
Scan title	List open ports on Google DNS ➡	List open ports on Google DNS ➡
Scan policy	List open ports (TCP/53,56,80,443,8080) ➡	List open ports (TCP/53,56,80,443,8080) ➡
Scan engine	NMAP - nmap-002	NMAP - nmap-002

PatrOwl Manager (1.0.0-BETA), 2018  

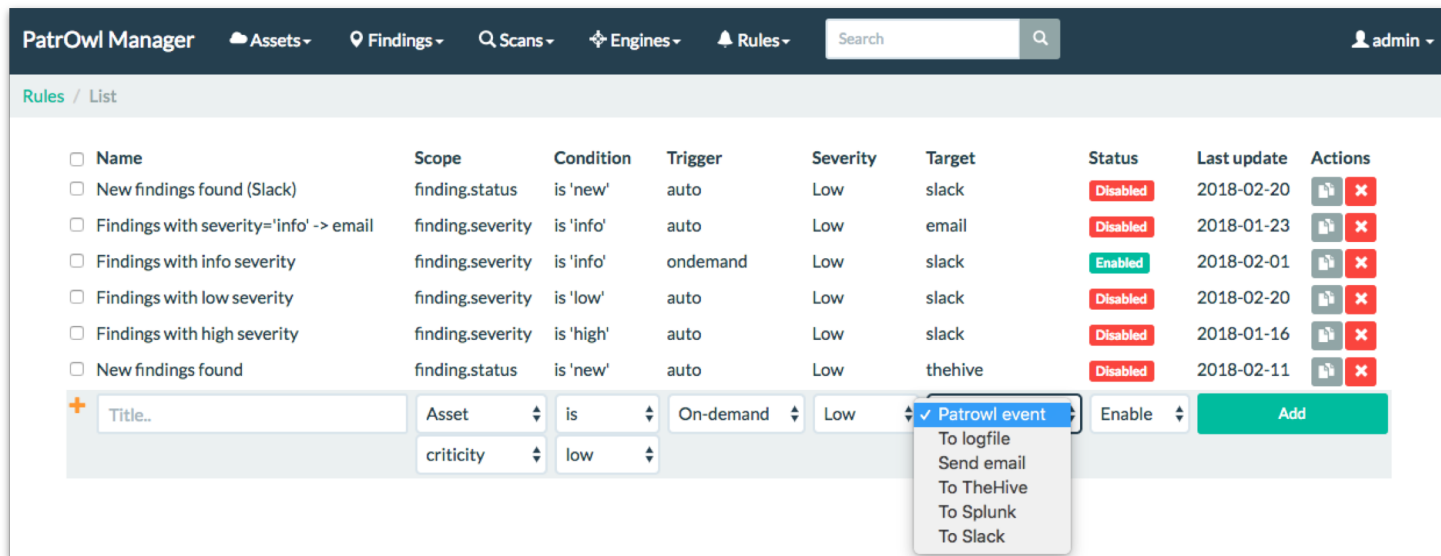
Engines status: 



# PatrOwl Manager - Alerting rules management view

Create, copy, modify or delete alerting rules

Change functional status



The screenshot displays the PatrOwl Manager interface for managing alerting rules. The top navigation bar includes links for Assets, Findings, Scans, Engines, and Rules, along with a search bar and a user profile icon labeled 'admin'. The main content area is titled 'Rules / List' and contains a table of existing rules. Below the table is a form to add a new rule, with a dropdown menu open for the 'Target' field.

Name	Scope	Condition	Trigger	Severity	Target	Status	Last update	Actions
<input type="checkbox"/> New findings found (Slack)	finding.status	is 'new'	auto	Low	slack	Disabled	2018-02-20	
<input type="checkbox"/> Findings with severity='info' -> email	finding.severity	is 'info'	auto	Low	email	Disabled	2018-01-23	
<input type="checkbox"/> Findings with info severity	finding.severity	is 'info'	ondemand	Low	slack	Enabled	2018-02-01	
<input type="checkbox"/> Findings with low severity	finding.severity	is 'low'	auto	Low	slack	Disabled	2018-02-20	
<input type="checkbox"/> Findings with high severity	finding.severity	is 'high'	auto	Low	slack	Disabled	2018-01-16	
<input type="checkbox"/> New findings found	finding.status	is 'new'	auto	Low	thehive	Disabled	2018-02-11	

<input type="checkbox"/> + Title..	Asset	is	On-demand	Low	<div>Patrowl event To logfile Send email To TheHive To Splunk To Slack</div>	Enable	<input type="button" value="Add"/>
	criticity	low					



# Contribution needed !!

Who's up for:

- **Test it** and give us **feedbacks !**
- **Contribute !**
  - New engines
  - Debug
  - Features ??

- **Joining the core team ?**
  - Dev[Sec]Ops, Security engineer, Cloud Architect, UX/UI Designer, QA Tester, Wonder-Woman (Batman is tolerated too) ...



## Q&A

**We have  
questions !?!**

**We want a  
demo !?!**

**Stop talking bro !  
We want  
a break now !?!**

## Contacts

More details ? Meet us ? Contributing ? Want a demo ? Want an awesome sticker ? Share a beer ? Requesting an online demo account (BETA test) ?

Find us everywhere on earth:

**Mail:** [getsupport@patrowl.io](mailto:getsupport@patrowl.io)

**Web:** <https://patrowl.io>

**Twitter:** [@patrowl\\_io](https://twitter.com/patrowl_io) (Follow us !)

**GitHub:** [@Patrowl](https://github.com/Patrowl) (Star and fork us !)